CLAIMS

What is claimed is:

1. A computerized method comprising:

defining a protection domain for a set of errors using an association between data and first integrity metadata, the protection domain to protect data traversing an input/output (I/O) datapath having a storage device and a first generation integrity point for a host as opposite endpoints; and

defining a first sub-domain nested within the protection domain using an association between the data and second integrity metadata, the first sub-domain to further protect data traversing a portion of the datapath having a second generation integrity point as an endpoint.

2. The computerized method of claim 1 further comprising:

defining a second sub-domain nested within the protection domain using an association between the data and third integrity metadata, the second sub-domain to further protect data traversing a portion of the datapath having a third generation integrity point as an endpoint.

3. The computerized method of claim 2, wherein the first and second sub-domains are nested in the protection domain as a hierarchy.

4. The computerized method of claim 2, wherein the third integrity metadata is operable to detect a subset of the set of data errors.

5. The computerized method of claim 1, wherein the first integrity metadata is operable to detect a first subset of the set of data errors.

6. The computerized method of claim 5, wherein the second integrity metadata is operable to detect a second subset of the set of data errors.

7. The computerized method of claim 6, wherein the first and second subsets together are operable to detect the set of data errors.

8. The computerized method of claim 1, wherein the portion of the datapath protected by the first sub-domain has one of the storage device and host as an opposite endpoint.

9. The computerized method of claim 1, wherein the set of data errors comprises bit corruption, misdirected I/O, and phantom I/O.

10. The computerized method of claim 1 further comprising:

detecting a data error within the protection domain using at least one of the first and second integrity metadata; and

identifying a portion of the I/O data path as a potential source of the data error.

11. The computerized method of claim 10, wherein detecting a data error comprises:

validating the data at one of the first and second integrity points.

12. The computerized method of claim 10 further comprising:

retrying a data transfer at the potential source of the data error.

13. The computerized method of claim 12 wherein retrying comprises:

resuming the data transfer using a replica.

14. The computerized method of claim 10 further comprising:

retrying a data transfer at an integrity point prior to the potential source of the data error.

15. The computerized method of claim 1, wherein a replication point is co-located with at least one of the first and second generation integrity points.

16. The computerized method of claim 1 further comprising:

establishing the first generation integrity point for the host; and

establishing the second generation integrity point for an intermediary component in the datapath.

17. A computer-readable medium having instructions to cause a processor to execute a method comprising:

defining a protection domain for a set of errors using an association between data and first integrity metadata, the protection domain to protect data traversing an input/output (I/O) datapath having a storage device and a first generation integrity point for a host as opposite endpoints; and

defining a first sub-domain nested within the protection domain using an association between the data and second integrity metadata, the first sub-domain to further protect data traversing a portion of the datapath having a second generation integrity point as an endpoint.

18. The computer-readable medium of claim 17, wherein the method further comprises:

defining a second sub-domain nested within the protection domain using an association between the data and third integrity metadata, the second sub-domain to further protect data traversing a portion of the datapath having a third generation integrity point as an endpoint.

19. The computer-readable medium of claim 18, wherein the first and second sub-domains are nested in the protection domain as a hierarchy.

20. The computer-readable medium of claim 18, wherein the third integrity metadata is operable to detect a subset of the set of data errors.

21. The computer-readable medium of claim 17, wherein the first integrity metadata is operable to detect a first subset of the set of data errors.

22. The computer-readable medium of claim 21, wherein the second integrity metadata is operable to detect a second subset of the set of data errors.

23. The computer-readable medium of claim 22, wherein the first and second subsets together are operable to detect the set of data errors.

24. The computer-readable medium of claim 17, wherein the portion of the datapath protected by the first sub-domain has one of the storage device and host as an opposite endpoint.

25. The computer-readable medium of claim 17, wherein the set of data errors comprises bit corruption, misdirected I/O, and phantom I/O.

26. The computer-readable medium of claim 17, wherein the method further comprises:

detecting a data error within the protection domain using at least one of the first and second integrity metadata; and

identifying a portion of the I/O data path as a potential source of the data error.

27. The computer-readable medium of claim 26, wherein detecting a data error comprises:

validating the data at one of the first and second integrity points.

28. The computer-readable medium of claim 26, wherein the method further comprises:

retrying a data transfer at the potential source of the data error.

29. The computer-readable medium of claim 28 wherein retrying comprises:

resuming the data transfer using a replica.

30. The computer-readable medium of claim 26, wherein the method further comprises:

retrying a data transfer at an integrity point prior to the potential source of the data error.

31. The computer-readable medium of claim 17, wherein a replication point is co-located with at least one of the first and second generation integrity points.

32. The computer-readable medium of claim 17, wherein the method further comprises:

establishing the first generation integrity point for the host; and

establishing the second generation integrity point for an intermediary component in the datapath.

33. An apparatus comprising:

means for defining a protection domain for a set of errors using an association between data and first integrity metadata, the protection domain to protect data traversing an input/output (I/O) datapath having a storage device and a first generation integrity point for a host as opposite endpoints; and

means for defining a first sub-domain nested within the protection domain using an association between the data and second integrity metadata, the first sub-domain to further

protect data traversing a portion of the datapath having a second generation integrity point as an endpoint.

34. The apparatus of claim 33 further comprising:

means for defining a second sub-domain nested within the protection domain using an association between the data and third integrity metadata, the second sub-domain to further protect data traversing a portion of the datapath having a third generation integrity point as an endpoint.

35. The apparatus of claim 34, wherein the first and second sub-domains are nested in the protection domain as a hierarchy.

36. The apparatus of claim 34, wherein the third integrity metadata is operable to detect a subset of the set of data errors.

37. The apparatus of claim 33, wherein the first integrity metadata is operable to detect a first subset of the set of data errors.

38. The apparatus of claim 37, wherein the second integrity metadata is operable to detect a second subset of the set of data errors.

39. The apparatus of claim 38, wherein the first and second subsets together are operable to detect the set of data errors.

40. The apparatus of claim 33, wherein the portion of the datapath protected by the first sub-domain has one of the storage device and host as an opposite endpoint.

41. The apparatus of claim 33, wherein the set of data errors comprises bit corruption, misdirected I/O, and phantom I/O.

42. The apparatus of claim 33 further comprising:

means for detecting a data error within the protection domain using at least one of the first and second integrity metadata; and

means for identifying a portion of the I/O data path as a potential source of the data error.

43. The apparatus of claim 42, wherein the means for detecting a data error comprises:

means for validating the data at one of the first and second integrity points.

44. The apparatus of claim 42 further comprising:

means for retrying a data transfer at the potential source of the data error.

45. The apparatus of claim 44 wherein the means for retrying comprises:

means for resuming the data transfer using a replica.

46. The apparatus of claim 42 further comprising:

means for retrying a data transfer at an integrity point prior to the potential source of the data error.

47. The apparatus of claim 33, wherein a replication point is co-located with at least one of the first and second generation integrity points.

48. The apparatus of claim 33 further comprising:

means for establishing the first generation integrity point for the host; and

means for establishing the second generation integrity point for an intermediary component in the datapath.